Mobile Device Policy

Background

Mobile devices are important tools for Alpha Response and their use is supported to achieve business goals. Alpha Response also realise that contact with some employees needs to be made outside the company, say in the event of a sick relative.

However mobile devices also represent a significant risk to information security and data security as, if the appropriate security applications and procedures are not applied, they can be a conduit for unauthorised access to the Alpha Response's data and IT infrastructure. This can subsequently lead to data leakage and system infection.

Alpha Response has a requirement to protect its information assets in order to safeguard our customers, intellectual property and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices.

General statement of policy

- Mobile phones or notebook computers may be used by only Alpha Response Directors or a person authorised in writing by an Alpha Response Director.
- Where there is a personal need for mobile phone contact, then the employee concerned shall discuss this with a Director. Use of the employee's phone in this situation shall not be a default solution.
- Mobile phones must use only Android 2.2 or later or IOS 10.x or later operating systems.
- Mobile phones are not allowed to be connected directly to the internal corporate network
- Devices must store all user-saved passwords in an encrypted password store.
- Devices must be configured with a secure password that complies with Alpha Response's password policy. This password must not be the same as any other credentials used within the organization.
- USB sticks must be encrypted and must not be taken off-site..

This policy shall be reviewed by a Director at least annually and recorded on 6.4 frmA.

Signed  Managing Director

Date 8/3/22.